Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of preventing piracy of a given software application ~~via a communication network, said method~~ comprising the steps of:

assigning a unique identification code to each authentic copy of such software application;

installing the software application in a data storage element on a user's computer;

configuring the software application to require service data to become fully functional;

requiring a user to enter into the user's computer personal data that identifies the user;

requiring the user to communicate user data over a communications network with a remote service system, the user data being derived, at least in part, from the personal data that identifies the user, and being derived, at least in part, from the unique identification code;

~~storably receiving~~ archiving user data received from the user over the communications network [on] in a data storage element of [a] the remote service system~~, for storably receiving said user data~~, said remote service system being connected to said communications network and designated to receive said user data;

~~associating said user data to archived data of said remote service system via element, of said remote service system, for processing~~ comparing received user data for each unique identification code with previously archived user data corresponding to the same unique identification code ~~, wherein said association event is initiated~~ to determine whether said user is pirating said software application;

selectively transmitting service data to ~~user system via element, of~~ the user's computer from said remote service system ~~, for transmitting said service data~~ when said remote service system determines that said service data should be transmitted, said user system being connected to said communications network and designated to storably receive said service data.

2. Canceled.

3. (Currently amended) The method as in Claim [2] 1,

wherein said user data comprises [of] ~~at least one program code sequence~~ the unique identification code that identifies said software application ~~stored~~ installed on a data storage element of [said user system] the user's computer.

4. (Currently amended) The method as in Claim [2] 1,

wherein said user data includes ~~identity information relating to said user of said software application~~ said personal data that identifies the user.

5. (Currently amended) The method as in Claim [2] 1,

wherein said user data includes product information relating to said software application ~~stored~~ installed on the data storage element of [said user system] the user's computer.

6. Canceled.

7. Canceled.

8. Canceled.

9. Canceled.

10. Canceled.

11. Canceled.

12. (Currently amended) The method as in Claim 1,

wherein said service data is ~~extracted from said archived data by element for processing said service data~~ is maintained in the data storage element of the remote service system.

13. (Currently amended) The method as in Claim 12,

wherein said service data comprises [of] at least one program code sequence that activates said software application stored on said data storage element of ~~said user system~~ the user's computer.

14. (Currently amended) The method as in Claim 12,

wherein said service data includes at least one program code sequence that results in a promotional message that may be displayed to said user ~~of said user system~~ on the user's computer system.

15. Canceled.

16. Canceled.

17. Canceled.

18. (Currently amended) The method as in Claim [15] 1,

wherein said service data [includes] is derived at least in part from said user data stored on said data storage element of said remote service system.

19. (Currently amended) The method as in Claim 1,

wherein the step of selectively transmitting said service data is an uploading event in which said service data is automatically transferred from said remote service system and storably received by ~~said user system via element, of said user system, for storably receiving said service data~~ the user's computer system.

20. (Currently amended) The method as in Claim 1,

wherein the step of selectively transmitting said service data is an uploading event in which said service data is manually transferred from said remote service system and storably received by ~~said user system via element, of said user system, for storably receiving said service data~~ the user's computer system.

21. (Currently amended) The method as in Claim 1,

wherein the step of selectively transmitting said service data is a downloading event in which said service data is made available to said user from said remote service system, and wherein said user ~~being able to download~~ downloads said service data into ~~said user~~ the user's computer system ~~via element, of said user system, for storably receiving said service data~~.

22. (Currently amended) The method as in Claim 1,

wherein [,] said software application includes a program code sequence that identifies said software application stored on said storage element of ~~said user~~ the user's computer system, said software application additionally being responsive to a second program code sequence that activates said software application, and which is transmitted to ~~said user~~ the user's computer system via said communications network.

23. (Currently Amended) A system for preventing piracy of a given software application ~~via a communications network~~, said software application having a unique identification code associated therewith, and said software application requiring service data to render said software application completely functional, said system comprising:

a user computer system on which a user desires to operate the software application, said user system being connected to a communications network ~~and designated by a user~~ to transmit user data and to storably receive said service data, ~~said user system including computer processor element, data storage element for storing data, element for transmitting user data, and element for storably receiving said service data~~ said user data being derived at least in part from personal data entered by the user on

the user computer system which identifies the user, and being derived at least in part from said unique identification code [.] ;

a remote service computer system connected to said communications network ~~and designated by the remote service provider~~ to storably receive ~~said~~ user data received over the communications network from the user computer system ~~and selectively transmit said service data, said remote service system including computer processor element, data storage element for storing data, element storably receiving said user data, element for detecting said user data, element for processing said user data, element for processing said service data, and element~~ said remote service computer system [for] transmitting said service data to said user computer system over said communications network when said remote service computer system determines that said user is not pirating said software application.

24. (Currently amended) The system as in Claim 23 [,] wherein said remote service computer system includes a data storage element for archiving user data for each unique identification code, wherein said remote service computer system compares user data received from the user computer system to user data previously archived by said remote service computer system relative to the same unique identification code, and wherein said remote service computer system transmits said service data to said user computer system when said user data received by said remote service computer system is consistent with user data previously archived by said remote service computer system relative to the same unique identification code ~~said user data is detected by said remote service system via element, of said remote service system, for detecting said user data, said remove service system connected to said communications network and designated to detect said user data~~.

25. (Currently amended) The system as in Claim 23 [,]

wherein said service data is ~~extracted from said archived data by element for processing said service data~~ is maintained by said remote service computer system in the data storage element used to archive said user data.

26. (Currently amended) The system as in Claim 23 [,]

wherein said service data is generated from said archived user data ~~by element for processing said service data~~.

27. (Currently amended) The system as in Claim 23[,]

wherein ~~the steps for transmitting said service data is an uploading event in which~~ said service data is automatically transferred [from] by said remote service computer system and storably received by said user computer system ~~via element, of said user system, for storably receiving said service data~~.

28. (Currently amended) The system as in Claim 23[,]

wherein ~~the steps for transmitting said service data is an uploading event in which~~ said remote service computer system manually transfers said service data ~~is manually transferred~~ from said remote service computer system ~~and storably received by~~ to said user system ~~via element, of said user system, for storably receiving said service data~~.

29. (Currently amended) The system as in Claim 23 [,]

wherein ~~the steps for transmitting said service data is a downloading event in which~~ said said remote service computer system makes said service data ~~is made~~ available to said user from said remote service system, said user being able to download said service data into said user computer system ~~via element, of said user system,~~ for storably receiving said service data.

30. (Currently amended) The system as in Claim 23,

wherein said software application includes a program code sequence that identifies said software application stored on said data storage element of said user system, said software application additionally being responsive to a second program code sequence that activates said software application, and which is transmitted to said user system via a communications network.

31. (New) A method of preventing piracy of a given software application comprising the steps of:

assigning a unique identification code to each authentic copy of such software application;

installing the software application in a data storage element on a user's computer;

configuring the software application to require service data to become fully functional;

requiring a user to enter into the user's computer personal data that identifies the user;

requiring the user to communicate user data over a communications network with a remote service system, the user data being derived, at least in part, from the personal data that identifies the user, and being derived, at least in part, from the unique identification code;

examining user data received by the remote service system from the user' computer to determine whether the user is pirating the software application;

selectively transmitting service data to the user's computer from said remote service system when said remote service system determines that the user is not pirating the software application; and

storably receiving the transmitted service data within the data storage element of the user's computer to render the software application fully functional.

32. (New) The method recited by claim 31 further including the step of archiving user data received from users over the communications network in a data storage element of the remote service system, and wherein said examining step includes the step of comparing received user data for each unique identification code with previously archived user data corresponding to the same unique identification code to determine whether said user is pirating said software application.